IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

ALLEGHENY COUNTY AIRPORT AUTHORITY, Plaintiff, v. **INVOLTA, LLC**, Defendant.	Civil Action No. 2:20-cv-1220 **JURY TRIAL DEMANDED**

COMPLAINT

The Allegheny County Airport Authority ("ACAA"), through its undersigned counsel at the law firm of Saul Ewing Arnstein & Lehr LLP, hereby files this Complaint against Involta, LLC ("Involta"), alleging as follows:

NATURE OF THE CASE

1. This case arises from Involta's breach of its contractual obligations to provide ACAA with information technology ("IT") and cybersecurity services for ACAA's computer systems, as well as Involta's negligence in providing these professional services.

2. Involta made serious errors and omissions when performing and completing its IT obligations (such as network management and installing, configuring, and upgrading software and servers) under the relevant contract, resulting in material breaches of that contract.

3. Involta then compounded its breaches by failing to detect and remediate cybersecurity vulnerabilities it created or allowed to persist because it failed in its cybersecurity obligations (such as conducting penetration tests, resolving vulnerabilities identified in its vulnerability scans, managing and testing ACAA's disaster recovery site, and patching software and servers) under the relevant contract.

4. These errors and omissions both breached the contract and negligently fell below professional IT standards used by the relevant certifying bodies, resulting in ACAA incurring significant losses, costs, and expenses (including retaining third-party IT, network, and cybersecurity consultants to audit and address the IT and network issues and cybersecurity vulnerabilities).

5. Involta has contractually agreed to indemnify ACAA for such losses, and it has refused to do so in full to date.

6. ACAA seeks to recover from Involta the substantial damages ACAA incurred due to Involta's negligence and multiple breaches of its contractual obligations.

PARTIES

7. Plaintiff ACAA is a municipal authority organized under the laws of the Commonwealth of Pennsylvania and headquartered in Pittsburgh, Pennsylvania.

8. ACAA operates the Pittsburgh International Airport ("PIT"), which serves several million passengers each year and is designated as federal critical infrastructure and is subject to significant physical and cyber security regulations and guidance under the Department of Homeland Security ("DHS"), Transportation Security Administration ("TSA"), and Federal Aviation Administration ("FAA").

9. ACAA also operates the Allegheny County Airport ("AGC"), which is designated by the FAA as the primary reliever airport for PIT in addition to handling corporate-jet and private-pilot air traffic.

10. Defendant Involta is a limited liability company organized under the laws of the State of Iowa, having its principal place of business in Cedar Rapids, Iowa.

11. Upon information and belief, Involta is considered a licensed professional with offices in Cedar Rapids, Iowa. Upon information and belief, Involta also employs, supervises, and is directly responsible for (under both corporate-liability and vicarious-

liability theories) a presently unknown number of licensed professionals and nationally certified information-technology professionals whose acts, errors, and omissions gave rise to the claims in this lawsuit. Among other things, Plaintiff is asserting a professional liability claim against Involta and reserves all rights to amend this Complaint to add "John Doe" or specifically named defendants when the licensing and certification statuses of specific Involta personnel becomes known to ACAA in discovery.

12. Involta is a provider of managed IT services and cybersecurity consulting to customers throughout the United States.

13. In 2015, Involta purchased substantially all of the assets of Data Recovery Services, LLC ("DRS") and agreed to be responsible for all obligations and liabilities that DRS had to ACAA when obtaining an assignment of ACAA Contract #3057, which was a 2013 agreement for DRS to provide ACAA with managed information-technology services at PIT and AGC in 2014.

14. A true and correct copy of ACAA Contract #3057 is attached under seal as Exhibit 1.

15. ACAA's acknowledgment and consent of the assignment of ACAA Contract #3057 from DRS to Involta is attached as Exhibit 2.

16. ACAA and Involta are parties to four change-order contract modifications that essentially extend the term and cost of ACAA Contract #3057.

17. True and correct copies of each change-order contract modification are attached under seal as follows:

a. Exhibit 3 – Extends Contract #3057 through 2015 and raises its value to $428,400

b. Exhibit 4 – Extends Contract #3057 through 2016 and raises its value to $661,400

c. Exhibit 5 – Extends Contract #3057 through 2017 and raises its value to $936,400

d. Exhibit 6 – Extends Contract #3057 through 2018 and raises its value to $1,221,400

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332. Complete diversity of citizenship exists between ACAA (a citizen of the Commonwealth of Pennsylvania) and Involta (a citizen of the State of Iowa). Additionally, the amount in controversy, exclusive of interest and costs, exceeds $75,000.

19. This Court has personal jurisdiction over Involta pursuant to the provision of Contract #3057 titled "Applicable Law," by which Involta agreed that "This Agreement shall be deemed to have been made in…Pennsylvania[.]" Additionally, Involta has 24/7/365 operations in Pennsylvania and has expressly marketed to numerous entities within Pennsylvania.

20. Venue is proper in this Court in accordance with 28 U.S.C. § 1391(b)(2) because a substantial part of the events (*e.g.*, the making of Contract #3057, the provision of services at PIT and AGC) and omissions giving rise to the claims occurred in and around Pittsburgh, Pennsylvania.

21. Pursuant to the provision of Contract #3057 titled "Applicable Law," ACAA and Involta further agreed that Contract #3057 "shall be construed in accordance with the laws of the Commonwealth of Pennsylvania."

FACTUAL BACKGROUND

A. Contract #3057 Obligates Involta to Provide a Variety of Services to ACAA.

22. Contract #3057 required Involta to supply ACAA from January 1, 2014 through December 31, 2018 with various IT and cybersecurity services; a non-exhaustive

list of examples of these services is set forth in paragraphs 23 through 26, below.

23. For instance, among the IT services that Involta was required to perform was hardware maintenance and software support for the servers used by ACAA and named in the Contract #3057 proposal materials at Exhibits 1 & 3-6.

24. Contract #3057 also required Involta to provide IT support to ACAA end-users of "virtual machine" or "cloud" software.

25. Contract #3057 also required Involta to perform cybersecurity services, including monitoring and "patching" (installing software updates to resolve security vulnerabilities identified since the software's initial launch) the computers and software used by ACAA.

26. Contract #3057 further required Involta to perform, on a quarterly basis, the cybersecurity services of vulnerability scans and "penetration testing," where Involta runs computer network scans and tries to test ACAA computers and networks to determine if vulnerabilities exist that could be exploited by nefarious parties to unlawfully access ACAA systems, devices, or data.

27. Throughout the contract-related documents, Involta routinely represented that it provided these "professional services" with "the highest level of technical expertise" by using "certified personnel" with "CISSP [*Certified Information Systems Security Professional*] [and] CISA [*Certified Information Systems Auditor*]" certifications, among other highly relevant certifications (not specifically named here to avoid publicly revealing details of ACAA's critical infrastructure). (*See* Exhibit 1 at 17; Exhibit 3 at 3; Exhibit 4 at 3; Exhibit 5 at 3; Exhibit 6 at 3.)

28. Involta also routinely represented that it would "manage a client's end point (excluding mobile devices) with virus protection[,]" "us[e] industry standard monitoring tools[,]" and "perform Critical and Security Operating System patches as provided by the

manufacturer under the customer's maintenance or availability plan." (Exhibit 6 at 10.)

B. Involta Committed Serious Errors and Omissions in Providing Services to ACAA.

29. In or around 2015, and unbeknown to ACAA at that time, Involta began to deliver to ACAA services that failed to meet industry standards.

30. Specifically, Involta omitted or neglected to conduct hardware maintenance or software support on many of the servers used by ACAA.

31. Involta further omitted or neglected to provide end-user support for many of the virtual machines or cloud software used by the ACAA.

32. Involta committed a number of errors and omissions when providing monitoring and "patching" services for many of the computers and software used by ACAA. Involta contractually agreed to install and manage periodic software updates that resolve security vulnerabilities that are identified after software is released. Installing software updates in a timely manner prevents malicious actors seeking to bypass airport security measures from using widely publicized vulnerabilities. Despite Involta's contractual obligation to install patches and updates in a timely fashion, Involta allowed outdated and unpatched software to remain in use at ACAA for excessive periods of time, and Involta left known vulnerabilities unpatched.

33. Upon information and belief, Involta knew since 2016 that it was erring in patching many of the computers and further knew that it was omitting patches from other computers altogether. These errors and omissions introduced significant, avoidable vulnerabilities into ACAA's network and systems.

34. Involta also negligently failed to activate antivirus software on the majority of ACAA's servers. Antivirus software is a type of industry standard tool used to prevent, detect, and remove malware and other computer threats. Involta's failure to activate the antivirus software created an unreasonable risk to ACAA's network and systems.

35. Involta made serious errors and omissions in failing to manage ACAA's end points with virus protection, in failing to use industry standard monitoring tools, and in failing to implement Critical and Security Operating System patches as provided by the manufacturer under the customer's maintenance or availability plan.

36. Involta further failed to perform a category of critical cybersecurity work: despite being required under the contract extensions in 2017 and 2018 (*see* Exhibits 5 and 6) to perform quarterly vulnerability scans and penetration tests, Involta in fact failed to carry out many of the vulnerability scans and *any* penetration testing. Additionally, Involta failed to advise and recommend remediation in a professional or workmanlike manner for most of the vulnerabilities identified in the vulnerability scans.

37. In addition to simply *not providing* penetration-testing services that it continued to bill and receive payment for, Involta did not provide ACAA with appropriate written recommendations to mitigate or remediate identified vulnerabilities from the few vulnerability scans it did.

38. Involta also committed a number of errors and omissions relating to ACAA's ability to recover data in the event of a disaster. Involta had been providing disaster recovery services to ACAA since at least November 2014, when Involta prepared an "ACAA Disaster Recovery Plan" for ACAA. During the final contract extension in 2018, ACAA contracted with Involta for disaster recovery services. Specifically, Involta agreed to manage and test the ACAA disaster recovery site (*i.e.*, a business-continuity solution that enables recovery of files, data, and applications following a cybersecurity incident, network disruption, natural or manmade disaster, or other data loss). (*See* Exhibit 6 at 2.)

39. Involta failed to manage and test the ACAA disaster recovery site, including failing to ensure the disaster-recovery site could back-up and restore all servers on ACAA's network. Had Involta tested the disaster recovery site, the results would have revealed that

the system could not accommodate anything more than e-mail in the event of a disaster.

40. Involta ran at least five vulnerability scans from 2016 to 2018 (though Contract #3057 called for at least ten scans during this time), but Involta misrepresented the results of the vulnerability scans and failed to resolve the majority of the vulnerabilities uncovered in the scan results.

41. Involta further was unable to provide ACAA with any evidence or documentation that Involta prepared for or attempted any other vulnerability scans or penetration tests.

42. ACAA was unaware of Involta's errors and omissions until a third-party cybersecurity audit in November 2018 identified them in dramatic fashion.

43. ACAA expected to receive high marks on its network's cybersecurity hygiene based on Involta's representations and assurances that Involta's certified IT and cybersecurity personnel would provide the professional IT and cybersecurity services to maintain and secure ACAA's network and infrastructure with the highest level of technical expertise.

44. The specific errors and omissions committed by Involta are so severe that the third-party cybersecurity firm (and its lead CISSP) marked the results of its audit as controlled under 49 CFR parts 15 and 1520 (addressing Sensitive Security Information and requiring approval from TSA and the Department of Transportation ("DoT") to disclose to a person without a "need to know").

45. The United States Department of Homeland Security ("DHS") also conducted a validated architecture design review of ACAA's network and found critical errors in the work that was solely the responsibility of Involta. (This audit will be made available under seal to this Court and Involta by ACAA upon appropriate clearance and a redacted version being received from DHS.)

46. Involta's errors and omissions fall so far below the standard expected of trained IT professionals such that well-known software companies have published publicly available step-by-step instructions explaining how to resolve them.

47. To the extent that this case sounds in professional negligence under Pennsylvania law and procedure addressing specific licensed or certified professionals, ACAA has attached its counsel's Certificate of Merit and will produce a related declaration from its third-party cybersecurity auditor (and other qualified IT professionals if needed) if appropriate protective orders and sealing orders are put into place by this Court. The Certificate of Merit is attached as Exhibit 7.

48. Yet, some of Involta's errors and omissions are so basic that even untrained consumers would recognize the issue—for instance, using outdated password protocols; using outdated software with publicly known vulnerabilities that is no longer supported by its manufacturer; using servers at or past their end of life; failing to manage and test the disaster recovery site; and failing to activate antivirus software on the majority of ACAA's servers.

49. When confronted with the results of the third-party cybersecurity audit, Involta admitted that it *never* ran a penetration test under Contract #3057—even though the terms of Contract #3057 called for Involta to run at least *eight* penetration tests over the term of Contract #3057 and Involta accepted payment for these services not rendered.

50. Involta did not provide its "professional services" in conformance with the minimum standards set by the certifying bodies for the CISSP and CISA certifications, or other relevant industry certifications.

51. The services promised by Involta in Contract #3057 are standard IT services that are understood by IT professionals to require a certain standard of care, particularly when provided by someone with the relevant technical certifications (*e.g.*, CISSP, CISA).

By way of example, the Information Systems Audit and Control Association ("ISACA"), which offers four professional IT and security certifications including CISA, requires certification holders to abide by its Code of Professional Ethics. The ISACA Code of Professional Conduct mandates certification holders to "perform their duties with objectivity, due diligence, and professional care, in accordance with professional standards." ISACA certification holders face disciplinary measures (including certification loss) for failure to comply with the Code of Professional Ethics.

52. Of the $1,221,400 that Involta earned under Contract #3057, at least $795,700 was paid for work that was performed with serious errors or omissions.

C. ACAA Undertook Extensive Remediation Efforts to Mitigate Damages as a Direct Consequence of Involta's Errors and Omissions.

53. Not only was ACAA deprived of the benefit of its contractual bargain when it did not receive the services it paid for, but also ACAA incurred substantial remediation costs to mitigate Involta's breach and protect its critical operations.

54. To address the serious failings and vulnerabilities resulting from Involta's errors and omissions, ACAA engaged several third-party vendors to perform substantial remediation work to bring Involta's work into conformance with commercially accepted cybersecurity and network hygiene standards, which resulted in an additional cost of approximately $700,000 to ACAA.

55. The third-party vendors corrected a number of Involta's errors and omissions, including patching software and validating compliance with cybersecurity regulations; performing penetration testing; establishing functional disaster recovery infrastructure, and remediating network stability and security issues identified in the audit.

56. Furthermore, ACAA's own employees spent approximately 5,000 hours on remedial efforts to mitigate the damages caused by Involta, which resulted in at least an additional $325,000 of loss to ACAA in addition to delays on other projects to which these

employees would have otherwise been assigned.

57. ACAA has demanded that Involta provide reimbursement for the damages ACAA incurred due to Involta's errors and omissions, but Involta has refused to provide reimbursement.

58. Involta specifically agreed to first-party indemnity in Contract #3057 and its change orders, with the relevant language being "The Consultant shall indemnify [and] protect…the Authority…from and against any and all…losses, damages…costs, and expenses…which the [Authority] may sustain, incur or suffer…arising out of, the negligent acts, errors, omissions or willful misconduct of Consultant[.]" (Exhibit 1 at § 4.A.)

59. Contract #3057 does not limit Involta's financial liability for breach or its indemnity obligation for negligence in any way by disclaiming consequential damages, professional negligence, or other relevant legal issues.

60. ACAA's damages may further increase, as ACAA continues to mitigate various errors and omissions that were caused by Involta.

D. Involta Engaged in a Lengthy and Dilatory Review of ACAA's Claims Through Involta's Insurer.

61. ACAA attempted in good faith to resolve its dispute with Involta for nearly two years, from October 2018 to August 2020.

62. During this time, ACAA met with and provided Involta with information and documents in response to numerous, and often duplicative, requests from Involta, its insurer, and its multiple lawyers.

63. ACAA prepared and transmitted a detailed demand letter in September 2019 to Involta.

64. While Involta's insurer already had counsel on the case—and that counsel acknowledged receiving the demand letter and promised a substantive response in October 2019—no substantive reply was received for 9 months until a change of Involta's counsel

occurred and voluntary mediation occurred at Involta's request on June 1, 2020.

65. Despite the efforts of Involta's new counsel, Involta and its insurer nonetheless continued to demonstrate an unwillingness to respond in timely and meaningful ways.

66. These actions by Involta and its insurer directly resulted in ACAA incurring attorney's fees and additional costs in an amount to be proven at trial.

COUNT I – Breach of Contract
Breach of Contract Pursuant to Contract #3057
(Errors and Omissions with IT Services)

67. The allegations set forth in each and every preceding paragraph are incorporated herein by reference.

68. ACAA and Involta are parties to a binding contract, Contract #3057.

69. ACAA has fully performed its obligations under Contract #3057.

70. Contract #3057 required Involta to provide to ACAA IT services that included hardware maintenance, software support, and virtual-machine support and that met certain quality and scope specifications.

71. Involta breached Contract #3057 by providing services that failed to meet quality and scope specifications because of Involta's own errors and omissions during the provision of such services.

72. As a direct and proximate result of Involta's breach, ACAA lost the value of the services for which it paid Involta and further was forced to incur significant additional mitigation/remediation costs on an urgent basis to protect federal critical infrastructure.

73. As a direct and proximate result of Involta's breach of contract, ACAA has suffered damages in an amount well in excess of $75,000 to be proven at trial.

COUNT II – Breach of Contract
Breach of Contract Pursuant to Contract #3057
(Errors and Omissions with Cybersecurity Services)

74. The allegations set forth in each and every preceding paragraph are incorporated herein by reference.

75. ACAA and Involta are parties to a binding contract, Contract #3057.

76. ACAA has fully performed its obligations under Contract #3057.

77. Contract #3057 required Involta to provide to ACAA cybersecurity services that met certain quality and scope specifications, including that the services rendered include robust monitoring and patching of computers and software, along with quarterly vulnerability scans and penetration testing.

78. Involta breached Contract #3057 by providing services that failed to meet quality and scope specifications because of Involta's own errors and omissions during the provision of such services.

79. As a direct and proximate result of Involta's breach, ACAA lost the value of the services for which it paid Involta and further was forced to incur significant additional mitigation/remediation costs on an urgent basis to protect federal critical infrastructure.

80. As a direct and proximate result of Involta's breach of contract, ACAA has suffered damages in an amount well in excess of $75,000 to be proven at trial.

COUNT III – Breach of Contract
Breach of Contract Pursuant to Contract #3057
(Indemnification)

81. The allegations set forth in each and every preceding paragraph are incorporated herein by reference.

82. ACAA and Involta are parties to a binding contract, Contract #3057.

83. ACAA has fully performed its obligations under Contract #3057.

84. Contract #3057 required Involta to indemnify ACAA for such losses,

damages, costs, and expenses arising from Involta's negligent acts.

85. Involta breached Contract #3057 by refusing to indemnify ACAA in full to date.

86. As a direct and proximate result of Involta's breach, ACAA lost the value of the contractual indemnity (*e.g.*, the service and remediation costs) promised by Involta and further was forced to incur significant additional legal fees, lost employee time, and other costs over the course of a nearly two-year effort to obtain indemnification that should have been provided much earlier.

87. As a direct and proximate result of Involta's breach of contract, ACAA has suffered damages in an amount well in excess of $75,000 to be proven at trial.

COUNT IV – Professional Negligence

88. The allegations set forth in each and every preceding paragraph are incorporated herein by reference.

89. Involta—and its personnel providing services to ACAA—had a duty imposed by their professional relationship with ACAA to have, use, and exercise the same knowledge, skill, and care that is ordinarily possessed, used, and exercised by others in the field of managed information-technology services and cybersecurity-consulting services.

90. Involta routinely represented that it provided managed IT services and cybersecurity consulting services to ACAA with "the highest level of technical expertise" by using "certified personnel" with CISSP and CISA certifications, among other certifications. (*See, e.g.*, Exhibit 5 at 3.)

91. Consistent with ordinary and customary business practices for entities that do not have certified professionals in specific technical areas on staff, ACAA contracted out certain IT functions to Involta.

92. ACAA hired and legally relied on Involta to provide skills, expertise, and

certified IT and cybersecurity professionals to manage ACAA's IT systems and network infrastructure, and the security of those systems.

93. Through its negligence—including that of its personnel—Involta breached these duties to ACAA and directly and proximately caused ACAA to sustain losses, injuries, and damages.

94. All of the resultant losses, damages, and injuries sustained were the direct and proximate result of the negligence, carelessness, or reckless indifference of Involta, including the following:

a. Involta omitted or neglected to conduct hardware maintenance or software support on many of the servers used by ACAA.

b. Involta further omitted or neglected to provide end-user support for the virtual-machine environment.

c. Involta erred in monitoring and "patching" many of the servers, computers, and software used by ACAA.

d. Involta designed and maintained a "disaster recovery" backup system that was incapable of performing its intended function.

e. Upon information and belief, Involta knew since 2016 that it was erring in its delayed and incomplete patching of much of ACAA's systems and software and further knew that it was omitting patches from other systems and software altogether.

f. Involta further failed to conduct many of the vulnerability scans and any quarterly penetration testing required under Contract #3057.

g. On information and belief, Involta failed to resolve any of the vulnerabilities uncovered in the results of the vulnerability scans it did conduct.

95. Involta's breach of its duty was with reckless indifference to the

vulnerabilities it created and/or perpetuated, and to the potential risks and harm to federally-designated critical infrastructure.

96. As a direct and proximate result of Involta's breach of duty, ACAA has suffered damages in an amount well in excess of $75,000 to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, ACAA hereby demands the following relief against Involta:

(a) Actual direct damages;

(b) Actual consequential damages;

(c) Punitive damages;

(d) Attorneys' fees and costs;

(e) Prejudgment and post-judgment interest; and

(f) Such other legal and equitable relief as this Court may deem just and proper.

JURY DEMAND

ACAA demands a trial by jury on all matters triable by jury.

SAUL EWING ARNSTEIN & LEHR LLP

/s/ Joseph A. Valenti
Joseph A. Valenti (Pa. ID 306788)
April F. Doss (*pro hac vice admission pending*)
Jillian K. Walton (Pa. ID 328389 *pro hac vice admission pending*)
SAUL EWING ARNSTEIN & LEHR LLP
One PPG Place, Suite 3010
Pittsburgh, PA 15222
Telephone: (412) 209-2500
Facsimile: (412) 209-2570

Attorneys for Allegheny County Airport Authority